COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL TRADE COMMISSION

In the Matter of Compete, Inc.

"FTC File No. 102 3155"

November 19, 2012

By notice published on October 29, 2012, the Federal Trade Commission ("FTC") has proposed a consent agreement with Compete, Inc. that would settle "alleged violations of federal law prohibiting unfair or deceptive acts or practices or unfair methods of competition."[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to ensure that the final order adequately protects the privacy of Compete users.

EPIC is a public interest research center located in Washington, D.C. EPIC focuses on emerging privacy and civil liberties issues and is a leading consumer advocate before the FTC. EPIC has a particular interest in protecting consumer privacy, and has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[2] EPIC's 2010 complaint concerning Google Buzz provided the basis for the Commission's investigation and October 24, 2011 subsequent settlement concerning

[1] Compete, Inc., Analysis of Proposed Consent Order to Aid Public Comment, 77 Fed. Reg. 65,550 (proposed Oct. 29, 2012), http://www.gpo.gov/fdsys/pkg/FR-2012-10-29/pdf/2012-26464.pdf.

[2] *See, e.g.*, Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., *FTC* File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html.

the social networking service.[3] In that case, the Commission found that Google "used deceptive tactics and violated its own privacy promises to consumers when it launched [Buzz]."[4] The Commission's settlement with Facebook also followed from a Complaint filed by EPIC and a coalition of privacy and civil liberties organization in December 2009 and a Supplemental Complaint filed by EPIC in February 2010.[5]

With regard to Compete, EPIC supports the proposed Consent Order. The Consent Order contains important privacy and security protections for consumers. However, EPIC urges the Commission to (1) strengthen the Order by requiring Compete to implement Fair Information Practices similar to those contained in the Consumer Privacy Bill of Rights; (2) make Compete's independent privacy assessments publicly available; (3) clarify the scope of implicit deception in the context of privacy policies; and (4) develop a best practices guide for anonymization techniques.

I. The Commission's Complaint Against Compete

The Complaint alleges that Compete used unfair and deceptive trade practices to secretly collect the personal information of consumers and failed to employ adequate security measures.[6] Compete accomplished this tracking through the Compete Toolbar, which claimed to allow consumer to "get 'instant access' to information about websites as they surfed the Internet" and

[3] Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), http://ftc.gov/opa/2011/03/google.shtm ("Google's data practices in connection with its launch of Google Buzz were the subject of a complaint filed with the FTC by the Electronic Privacy Information Center shortly after the service was launched.").
[4] *Id.*
[5] In the Matter of Facebook, Inc., (2009) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf [hereinafter EPIC 2009 Facebook Complaint]; In the Matter of Facebook, Inc., (2010) (EPIC Supplemental Materials in Support of Pending Complaint and Request for
Injunction, Request for Investigation and for Other Relief), https://epic.org/privacy/inrefacebook/EPIC_Facebook_Supp.pdf [hereinafter EPIC 2009 Facebook Supplement]; In the Matter of Facebook, Inc., (2010) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) , https://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf [hereinafter EPIC 2010 Facebook Complaint].
[6] In the Matter of Compete, Inc., FTC File No. 102 3155 (2012) (Complaint), http://www.ftc.gov/os/caselist/1023155/121022competeinccmpt.pdf.

the Consumer Input Panel, which claimed to "allowed consumers to win rewards while expressing their opinions to companies about products and services."[7]

Specifically, Compete engaged in both explicit and implicit forms of deception. Compete explicitly stated that the data it collected was stripped of personally identifying information and anonymized through data aggregation and the assignment of a randomly-generated user ID.[8] According to the FTC, however, Compete's anonymization filters "were too narrow and improperly structured to avoid collecting [personally identifiable] data," and thus Compete could have collected personal IDs, security codes, or credit card numbers.[9] Compete also explicitly stated that it maintained reasonable security procedures while failing to do so, resulting in the transmission of information over the Internet in clear, readable text.[10]

Compete implicitly deceived consumers by omitting material information about the amount of personal information collected through its Consumer Input Panel and Toolbar. Compete stated that these services would collect, at most, consumers' browsing behavior.[11] These products collected far more information than a user's browsing activity, including "information about all websites visited, all links followed, and the advertisements displayed when the consumer was on a given web page [and] credit card numbers, financial account numbers, security codes and expiration dates, usernames, passwords, search terms, or Social Security numbers."[12]

Finally, the Complaint alleges that Compete's failure to implement and maintain reasonable security procedures was an unfair business practice.[13]

---

[7] *Id.* at ¶ 4
[8] *Id.* at ¶ 13-14
[9] *Id.* at ¶ 15
[10] *Id.* at ¶¶ 16-18
[11] *Id.* at ¶¶ 7-9
[12] *Id.* at ¶¶ 10-11
[13] *Id.* at ¶ 16, ¶¶ 26-27.

II. The Commission's Proposed Consent Order

Part I of the Order prohibits Compete from "directly or indirectly . . . [c]ollecting any information from any [Compete] Data Collection Agent" without first: (1) "prominently" informing consumers of the type of information that Compete will collect; and (2) "obtaining express affirmative consent from the consumer" to collect, use, and share consumer information.[14] Compete is also barred from using any consumer information "gathered on or after February 1, 2010" without consumers' express affirmative consent.[15] Compete can, however, use this consumer information without obtaining consent if it does so "in an aggregate and/or anonymous form that does not disclose, report, or otherwise share any individually identifiable information," and does not otherwise access consumer information.[16] Part I further prohibits Compete from making "any material change" to its data collection, use, or sharing practices without obtaining consumer express affirmative consent.[17]

Part II of the Order requires Compete to notify Affected Consumers of "the categories of personal information that were, or could have been" collected and transmitted through Compete software.[18] Compete must also inform Affected Consumers how to "permanently disable and/or uninstall" Compete software that collected personal information.[19]

Part IV prohibits Compete from making false and/or misleading representations about the extent to which it "collects, maintains and protects the security, privacy, confidentiality, or integrity of any information collected from or about consumers."[20]

---

[14] In the Matter of Compete, Inc., FTC File No. 102 3155 (2012) (Agreement Containing Consent Order) 4-5, http://www.ftc.gov/os/caselist/1023155/121022competeincagreeorder.pdf [hereinafter "Compete Proposed Consent Order"].
[15] *Id*. at 5.
[16] *Id*.
[17] *Id*.
[18] *Id*. at 6.
[19] *Id*.
[20] *Id*. at 7.

Part V of the Order requires Compete to implement and "maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of personal information collected from or about consumers."[21] The program must be "fully documented in writing" and appropriate for Compete's size and complexity, nature and scope of Compete's activities, and "sensitivity of the personal information collected from or about consumers."[22] Among other requirements, Compete's information security program must: (1) designate an employee to oversee the program; (2) identify material risks that could lead to "unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of personal information" and conduct a risk assessment on the sufficiency of safeguards; and (3) implement "reasonable safeguards to control the risks identified through risk assessment."[23]

Under Part VI, Compete must obtain initial and biennial assessments from a "qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession."[24] This person must be certified by an organization approved by the FTC.[25] The first report is due to the FTC 180 days after the Order takes effect; subsequent assessments are due every two years for the next 20 years.[26] The assessments must explain Compete's privacy safeguards and how they are appropriate to meet the Order's requirements.[27]

[21] *Id*.
[22] *Id*.
[23] *Id*. at 7-8.
[24] *Id*. at 8.
[25] *Id*.
[26] *Id*.
[27] *Id*. at 9.

Part VII requires Compete to delete or destroy any personally identifiable information in its "custody or control that was collected prior to February 1, 2010" within 14 days after the Order goes into effect.[28]

Pursuant to Part VIII, Compete must make available to the Commission any "dissemination of any representation covered by this [O]rder" for "a period of 5 years after the last date of dissemination."[29] Additionally, for a period of 3 years after each independent Assessment required under Part VI of the Order, Compete must make available "all materials relied upon to prepare the Assessment."[30]

Parts IX through XI contain various procedural details and requirements, such as the requirement that Compete deliver a copy of the Order to officers and directors who have responsibilities relating to the subject matter of the Order, and the provision that terminates the Order twenty years from the date of issuance, or twenty years from the most recent FTC complaint alleging a violation of the Order, whichever comes later.[31]

III. The Commission Should Amend its Policy Statement on Deception to Unequivocally Include Omissions Affecting Consumer Privacy

EPIC supports the Commission's finding of deception by omission in the present matter. Indeed, Compete's omissions concerning Compete software's performance and warranties regarding data collection were material. Equally important is Compete's omissions on privacy matters "likely to be considered important by consumers."

Under Section 5, deceptive omissions are material "if they significantly involve health, safety, or other areas with which the reasonable consumer would be concerned."[32] The

[28] *Id.*
[29] *Id.*
[30] *Id.* at 10.
[31] *Id.* at 10-11.
[32] FED. TRADE COMM'N, POLICY STATEMENT ON DECEPTION (1983), *available at*

Commission considers omissions concerning product or service cost, safety, purpose, efficacy, quality, durability, performance or warranties to be material.[33] Materiality can also include omissions "likely to be considered important by consumers."[34]

Numerous studies prove privacy is important to consumers. A recent survey by the Pew Research Center found that the majority of mobile phone users have uninstalled or avoided apps due to privacy concerns.[35] According to the report, 54% of mobile users have decided to not install an app after discovering the amount of information it collects, and 40% of mobile users uninstalled an app after discovering that it was collecting personal information that the user did not wish to share.[36] This poll follows another survey by Pew that found that users were becoming more active in managing their social media accounts due to privacy concerns.[37] And these surveys follow a host of research that reveals consumers consider privacy highly important, especially amid ever-evolving technology.[38] In light of the well-documented fact that consumers care about privacy, and that the Commission investigates material omissions affecting consumer privacy[39], the Commission should amend its Deception Policy to explicitly categorize omissions impacting consumer privacy as deceptive under Section 5. This clarification will inform

---

http://www.ftc.gov/bcp/policystmt/ad-decept.htm.
[33] *Id.*
[34] *Id.*
[35] Jan Lauren Boyles, Aaron Smith, Mary Madden, Pew Research Ctr., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES OVERVIEW, Sept. 5, 2012, http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx?utm_source=Mailing+List&utm_campaign=2251646e41-Mobile_privacy_09_05_2012&utm_medium=email.
[36] Jan Lauren Boyles, Aaron Smith, Mary Madden, Pew Research Ctr., PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES MAIN FINDINGS, Sept. 5, 2012, http://pewinternet.org/Reports/2012/Mobile-Privacy/Main-Findings/Section-1.aspx.
[37] Mary Madden, Pew Research Ctr., PRIVACY MANAGEMENT ON SOCIAL MEDIA SITES OVERVIEW, Feb. 24, 2012, http://www.pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx.
[38] *See, e.g.,* Josh Smith, *Privacy Trumps Cybersecurity, Polls Show*, NAT'L JOURNAL, (July 11, 2012, 6:56AM),http://www.nationaljournal.com/daily/privacy-trumps-cybersecurity-poll-shows-20120710; Consumers Union, *Consumer Report Poll:Americans Extremely Concerned About Internet Privacy* (Sept. 25, 2008), http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html; John B. Horrigan, *Cloud Computing Gains in Currency*, PEW INTERNET AND AMERICAN LIFE PROJECT (Sept. 12, 2008).
[39] *See, e.g.*, In the Matter of Google, Inc., FTC File No. 102 3136 (2012), http://ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf.

companies that they must notify consumers of all privacy policy changes, and that failure to do so will result in a finding of deception under Section 5.

IV. The Commission Should Issue a Best Practices Guide for De-Identification Techniques

Many companies claim to anonymize or de-identify personal information by aggregating it or assigning pseudonyms to it. Behavioral advertising companies routinely claim that the use of pseudonymous identifiers renders personal information anonymous.[40] Recently, Facebook's data-sharing arrangement with Datalogix relied on both pseudonymization (through the use of a hash function) and aggregation to allegedly anonymize personal information.[41] Data brokers also rely on the aggregate nature of their marketing data as a defense against criticism of their privacy practices.[42] And, of course, Compete claimed to use both aggregation and pseudonyms to render personal information anonymous.[43]

As the Compete case demonstrates, however, these claims of anonymization are often deceptive. Widely-publicized anonymization failures involving Microsoft,[44] Netflix,[45] and the

[40] *DMA Online Behavioral Advertising (OBA) Compliance Alert & Guidelines for Interest-Based Advertising*, DIRECT MARKETING ASSOC., http://www.dmaresponsibility.org/privacy/oba.shtml (last visited Nov. 19, 2012) ("Relevant Ads Using Anonymous Data. OBA relies on anonymous, aggregated data to deliver an ad to a computer based on the computer browser's activity, not the activities of a specific individual. Companies use cookies to make this happen." ").

[41] *How Does Facebook Partner with Outside Companies for Campaign Impact Measurement? How Does it Affect Me?*, FACEBOOK, https://www.facebook.com/help/211774365532736/ (last visited Nov. 19, 2012) (stating that Datalogix matches these users ""in a hashed format with the data [Datalogix] receives from [its] retail partners." and "As trusted service providers, these companies have been contracted to produce aggregate and anonymous measurement reports to advertisers.")"

[42] Katy Bachman, Lawmakers Open Data Broker Probe, ADWEEK (Jul. 25, 2012), http://www.adweek.com/news/advertising-branding/lawmakers-open-data-broker-probe-142185 (reporting that data brokers distinguished between themselves and credit reporting agencies in that """"That broad definition has the marketing industry both confused and alarmed since the direct marketing database companies aggregate information for marketers, while credit reporting firms provide precise consumer information.").

[43] Compl. ¶ 14 ("Further, we aggregate data on hundreds of thousands of users before supplying data to our clients, thereby ensuring that an individual's privacy remains intact at all times."); ¶ 13 ("In addition, as a member of Compete you are assigned a randomly generated user ID ensuring your anonymity").

[44] Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMESN.Y. TIMES (, Aug. 9, 2006), https://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all.

Massachusetts state government[46] have shown that even relatively sophisticated techniques have still permitted researchers to identify particular individuals in large data sets. The Commission has also recognized the limits of aggregation and pseudonyms as techniques of anonymization. The Commission's former Chief Technologist has written on the Commission's technology blog that "the casual assumption that hashing is sufficient to anonymize data is risky at best, and usually wrong"[47]; that "it's clear that pseudonyms are not 'anonymous' and that attaching a pseudonym to a user, or gathering information about a pseudonymous user over time, can impact privacy"[48]; and finally that "A common intuitions is aggregate data . . . is inherently free of privacy implications. As we'll see, that isn't always right."[49]

Given the problems associated with certain de-identification techniques, and the falsity of claiming that pseudonyms and aggregation necessarily render data anonymous, the Commission should issue a best practices guide to de-identification. EPIC favors techniques to de-identify user data,[50] and many scholars are performing valuable research on various de-identification techniques,[51] but greater clarification and standardization is needed.

---

[45] Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, in PROC. OF THEPROC. OF THE 2008 IEEE SYMP.SYMP. ON SECURITY AND PRIVACY ON SECURITY AND PRIVACY 111, *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.

[46] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* Uniqueness of Simple Demographics in the U.S. Population (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP34, 2000), *available at* http://dataprivacylab.org/projects/identifiability/paper1.pdf. Similar research has revealed the surprising degree to which the combination of birth date and geographic location allow for the prediction of Social Security numbers. *See* Alessandro Acquisti and Ralph Gross, *SSN Study: Frequently Asked Questions*, Heinz College of Carnegie Mellon University (July 2009), http://www.heinz.cmu.edu/~acquisti/ssnstudy/

[47] Ed Felten, *Does Hashing Make Data "Anonymous"?*, TECH@FTC (Apr. 22, 2012), https://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous.https://techatftc.wordpress.com/2012/04/22/does-hashing-make-data-anonymous/

[48] Ed Felten, *Are Pseudonyms "Anonymous"?* TECH@FTC (Apr. 30, 2012), https://techatftc.wordpress.com/2012/04/30/are-pseudonyms-anonymous/.

[49] Ed Felten, *Is Aggregate Data Always Private?* TECH@FTC (May 21, 2012), https://techatftc.wordpress.com/2012/05/21/is-aggregate-data-always-privat/.

[50] *See generally* Re-identification, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/reidentification/ (last visited Nov. 19, 2012).

[51] *See, e.g.*, Cynthia Dwork, Differential Privacy*: A Survey of Results*, in THEORY AND APPLICATIONS OF MODELS OF COMPUTATION 1, 3 (Manindra Agrawal et al. eds., 2008); *see also* Latanya Sweeney, *k-anonymity: A Model for*

Anonymization problems have long existed in the digital environment, and have even been the subject of previous Commission enforcement actions. In 1999, for example, the Commission sanctioned Liberty Financial for claiming to anonymously maintain personal information collected from a survey, despite "combin[ing] the personal identifying information that it collects in the Entry Form section of the survey, including name, address, and e-mail address, with all other survey responses."[52] Most recently in its 2012 privacy report, the Commission described anonymous data as information that is "not reasonably identifiable."[53] However, the Commission has not yet defined best practices for de-identification. Best practices would give businesses and consumer groups something more concrete against which to measure claims of de-identification and anonymity.

V. The Commission Should Require Compete to Implement the Fair Information Practices Outlined in the Consumer Privacy Bill of Rights

Earlier this year, the President set out a comprehensive framework for privacy protection– the Consumer Privacy Bill of Rights (CPBR) – that provides substantive privacy protections for users. [54] The CPBR enumerates seven principles: Individual Control, Transparency, Respect for Context, Security, Access and Accuracy, Focused Collection, Accountability.[55] These principles are central to the right of privacy, and appear in numerous frameworks, such as the Organization for Economic Cooperation and Development (OECD)

Protecting Privacy, INT'L J. ON UNCERTAINTY, FUZZINESS AND KNOWLEDGE-BASED SYSTEMS, 10(5), 2002; 557-570.

[52] *Liberty Financial Companies, Inc.*, FTC File No. 982 3522 (1999) (Complaint), *available at* http://www.ftc.gov/os/1999/08/libertycmp.pdf

[53] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 22 (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.FTC report 22

[54] *See* EXEC. OFFICE OF THE PRESIDENT, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012) [hereinafter "White House CPBR"].

[55] *Id*. at 10.

Privacy Guidelines[56] and the Privacy Act of 1974.[57] Several of these principles are also highlighted in the Commission's recent report, such as privacy by design, choice, and transparency.[58]

These principles would impose certain requirements on the collection and use of personal information in the social networking context. For example, Individual Control and Respect for Context would require that users consent to new uses or disclosures of their information, such as disclosure to a third-party advertiser. And Transparency and Access and Control would require that users be able to access all of the data that Compete keeps about them. The right to access increases awareness by giving users the ability to see the full extent of the data collected by a company. The right to access increases users' control by placing the locus of ownership closer to the user, who gains the ability to inspect data and take steps to correct errors. Transparency also would require the Commission to make Compete's privacy audits publicly available to the greatest extent possible.

The proposed Order promotes some of the CPBR's principles. For example, the Order requires Compete adhere to the Security principle because it orders Compete to provide privacy and security safeguards to control "unauthorized access, use, destruction, . . .modification . . .and improper disclosure."[59] Likewise, the proposed Order encourages Accountability to the FTC and consumers by requiring initial and biennial privacy audits on Compete's data collection, retention, and disclosure.[60] The Order should, however, further advance the CPBR by adhering

[56] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2.
[57] Privacy Act of 1974, 5 USC § 552a.
[58] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[59] White House CBPR, at 48; Compete Proposed Consent Order at 7-9.
[60] Compete Proposed Consent Order at 8-9.

to additional Fair Information Practices. Specifically, Part I should be revised so consumers can exercise individual control over which types of information Compete intends to collect and disclose. Although the Order requires Compete inform consumers of "all types of information that will be collected" and obtain consent before disclosing this information, the Order should permit Compete consumers to select which data Compete will collect and for what purposes Compete can disclose consumer data. As the Order is currently written, Compete simply informs consumers of the type of information it will collect; it does not permit consumers to decide which information Compete collects.[61] And the Order also does not grant consumers a right to access and ensure accuracy of the data that Compete maintains.

By granting Compete consumers control over their data, along with the rights to access and amend their personal information, the Order can more fully comply with CPBR's principals.

VI. The Commission Should Make Compete's Privacy Audits Publicly Available to the Greatest Extent Possible

The Commission has emphasized its commitment to transparency and oversight when adopting similar consent orders in the past. After finalizing a consent order with Google that required similar independent assessments, the Commission wrote to EPIC and stated that "[t] o the extent permissible under law, the public may have access to the submissions required pursuant to the order."[62] Similarly, regarding Facebook's privacy audits, the Commission said that "If the FTC determines that the assessments have been frequently requested or are likely to be frequently requested because of the their subject matter, the agency will post such portions as may be released to the public on the FTC's website."[63]

[61] *Id*. at 4-5.
[62] Letter from Donald S. Clark, Secretary, Fed. Trade Comm'n, to Marc Rotenberg et. al (Oct. 13, 2011), http://www.ftc.gov/os/caselist/1023136/111024googlebuzzepic.pdf.
[63] Letter from Donald S. Clark, Secretary, Fed. Trade Comm'n, to Commenters, 44 (July 27, 2012), http://www.ftc.gov/os/caselist/0923184/120810facebookcmbltrs.pdf .

Although companies may exempt trade secrets or confidential commercial information, similar audits containing extensive technical details have been released in their entirety, all without identifiable competitive harm. In 2009, Canadian Privacy Commissioner conducted an investigation of Facebook's privacy policies and released a 113-page report that described in detail the findings of the investigation and the office's recommendations.[64] More recently, the Irish Data Protection Commissioner's investigation into Facebook, cited above, produced a 150-page report and 77 pages of "technical analysis" that were made publicly available.[65] Furthermore, the initial compliance self-assessment should be made available without redactions, as was the case with Google's initial compliance report.[66] Thus, to facilitate public education and the transparency of the audit process, the Commission should make Compete's privacy audits publicly available.

IV. Conclusion

EPIC supports consent order in this case. However, consumers' privacy would be better protected by modifying the order to include FIPs and the other recommendations contained in these comments. EPIC therefore urges the Commission to adopt the changes to the proposed orders set out above.

[64] OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC) AGAINST FACEBOOK INC. (2009), http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm#complaint.
[65] *See* DATA PROTECTION COMM'R, REPORT OF AUDIT (2011), http://dataprotection.ie/documents/facebook%20report/report.pdf/report.pdf.
[66] Letter from Sarah Mathias, Associate General Counsel, Fed. Trade Comm'n, to Ginger McCall, Director, EPIC Open Gov't Program (Feb. 15, 2012), *available at* https://epic.org/privacy/ftc/google/EPIC-FTC-Google-Compliance-Reply-02-17-12.pdf.

Respectfully Submitted,

Marc Rotenberg, EPIC Executive Director
David Jacobs, EPIC Consumer Protection Counsel
Khaliah Barnes, EPIC Administrative Law Counsel
Electronic Privacy Information Center
1718 Connecticut Ave. NW Suite 200
Washington, DC 20009
202-483-1140 (tel)
202-483-1248 (fax)